

AFFIDAVIT OF PAUL F. HEALY

I, Paul F. Healy (herein referred to as "Affiant"), being a Special Agent of the Federal Bureau of Investigation, United States Department of Justice, and being properly sworn, state the following:

Background of Affiant

I am a Special Agent with the United States Department of Justice, Federal Bureau of Investigation, and have been so employed since 1997. I am presently assigned to the Federal Bureau of Investigation's Chattanooga Resident Agency in Chattanooga, Tennessee, and more specifically the Violent Crimes and Safe Streets Task Force. In the performance of my duties as a Special Agent I have conducted numerous investigations of auto theft, narcotics, bank robbery, internet fraud, computer intrusion, interstate transportation of obscene material, and other violations of federal law. During my tenure as a Special Agent for the Federal Bureau of investigation, I have been involved in the investigation of over 100 bank robberies and other violent crimes involving violations of both state and federal laws. I am currently the case agent for the bank robbery and use and carry of a firearm investigation (violations of Title 18 U.S.C. 2113(a) and (d) and Title 18 U.S.C. Section 924(c), respectively) described in detail below.

Locations to be Searched

This affidavit is in support of a Search Warrant for two laptop computers, an Acer laptop computer bearing serial number LXAKVOX3798080903E2503 and a Dell laptop computer bearing serial number CN-03U652486433930499, and a Tomtom GPS device bearing serial number C-NO:Y25497B00279 that were located in the vehicle of JONATHAN ALLEN and TERENCE CRAWLEY and seized incident to their arrest on January 04, 2010. CRAWLEY and ALLEN are incarcerated and awaiting trial. The information contained in this affidavit is based upon my own training and experience, my own knowledge and information provided to me by other law enforcement officers.

Overview and Chronology of Investigation

I. THE BANK ROBBERY

Just before 9:00 a.m. on January 4, 2010, two armed men entered the Citizen's Tri-County Bank (CTCB) located at 402 North Cedar Avenue, South Pittsburg, Tennessee, ordered the occupants to the floor, and announced, "this is a hold up." Bank employees described the gunmen as African American with one robber being taller than the other.

After entering the bank, the shorter gunman vaulted the teller counter, ordered the tellers to the floor, and began to rob the teller drawers while waving a black semi-automatic handgun and yelling at the tellers in profane language. The taller gunman rounded up the bank employees forcing them onto the floor and even dragging one woman over a desk. He then stood watch over them with a silver semi-automatic handgun. One CTCB employee who arrived late was prodded at gunpoint by the taller gunman into the bank's records vault and locked there.

While the taller gunman stood watch, the shorter gunman stuffed the money into a gym bag as he robbed each teller's drawer. He then rounded up employees who had keys to the bank vault and forced them to open it. He entered the vault with the employees, made them lie on the floor of the vault, and emptied the drawers of the various compartments. After receiving a signal from the taller gunman, the shorter gunman locked the employees in the vault. Then having stolen approximately \$70,865 from the CTCB, the gunmen left the bank and fled the scene in a green dodge Stratus. Affiant is aware the bank is federally insured.

The Stratus was ultimately found with the ignition running approximately three miles south of the bank in Jackson County, Alabama. The ignition column of the Stratus had been smashed so the vehicle could be hot wired, all of the visible vehicle identification number (VIN) plates had been removed or scratched in order to obfuscate the identity of the vehicle. The vehicle was identified via a confidential VIN and had been reported stolen in Fort Payne, Alabama, earlier on the morning of January 4, 2010. Inside the Dodge Stratus, investigators found two camouflage jackets, a torn pair of khaki pants and a pair of camouflage pants with \$440 in the front pocket.

II. THE TRAFFIC STOP

Affiant is aware that at approximately 4:45 PM that same day (January 04, 2010), Virginia State Police (VSP) Trooper Oris J. Lilly III, assisted by VSP Trooper Russell Edwards conducted a traffic stop on a Lexus sedan in the vicinity of Wytheville, Virginia, and subsequently searched the Lexus sedan occupied by Allen and Crawley. In the trunk of the Lexus, Trooper Lilly found the following:

a black nylon backpack containing approximately \$69,948 wrapped in CTCB bank bands

two handguns, i.e. a silver Ruger P-90 and a black High Point and ammunition in a secret compartment of the vehicle.

camouflage masks

a box for a Radio Shack scanner

several license plates (including a tag for Coffee County, Tennessee)

a card with the radio frequencies for Grundy and Marion County Sheriff's offices and the words "Grundy" and "Marion" written on it.

a jar labeled Sand Mountain's Famous Syrup Molasses (from Scotsboro, Alabama)

a pipe for smoking marijuana

digital scales

Acer laptop S/N LXAKVOX3798080903E2503

Dell laptop S/N CN-03U652486433930499

Tomtom GPS S/N C-NO:Y25497B00279

Meanwhile, Trooper Edwards continued with his search of the passenger compartment of the Lexus and discovered a ballistic vest under the passenger side floor mat. The Troopers also found a partially smoked marijuana cigarette, another \$62 in cash in the vehicle and \$395 in cash on the two men - for a total of \$70,405. In this cash were fifteen bait bills that had been stolen from the CTCB earlier that day. With the assistance of

the VSP Bureau of Criminal Investigations, the Troopers realized that Allen and Crawley might be the men who robbed the CTCB earlier that day. Accordingly, they were placed under arrest.

III. THE INTERNET AND DEFINITIONS OF TECHNICAL TERMS PERTAINING TO COMPUTERS

As part of my training and experience, as well as information obtained from discussions with other law enforcement officers with experience in cases involving computer use, I have become familiar with the Internet, which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet - for example, through a university, an employer, or a commercial service - which is called an "Internet Service Provider" or "ISP" (see definition of "Internet Service Provider" below). Once the individual has accessed the Internet, that individual can do a variety of things including visiting websites (see definition of "website" below), and make purchases from them.

Set forth below are some definitions of technical terms used within this Affidavit, pertaining to the Internet and computers more generally:

a. Internet Service Providers (ISPs) and the Storage of ISP Records: Internet Service Providers ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs may provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communication equipment. ISPs maintain records ("ISP record") pertaining to their subscribers (regardless of whether those subscriptions are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which

may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use.

b. Website: A website consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-Up language (HTML) and is transmitted from the web servers to various clients via the Hyper-Text Transport Protocol (HTTP).

c. Domain Name: Domain names are typically strings of alphanumeric characters, with each level delimited by a period that are associated with a unique Internet Protocol ("IP") addresses (defined below). For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Each level, read backwards - from right to left - further identifies parts of an organization. Examples of first level or top-level domain are typically .com for commercial organizations, .gov for the United States government, .org for organizations, and .edu for educational organizations. Second level names will further identify the organizations, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identified. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

d. Internet Protocol Address: Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. ISP's can employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up

customer. On the other hand, some ISPs employ static IP addressing, that is a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

e. Log file: Log files are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

IV. FORENSIC SEIZURE AND ANALYSIS OF COMPUTERS

Computer hardware, computer software, computer-related documentation, passwords, and data security devices may be important to a criminal investigation in three important respects: (1) as instrumentalities for the violations of federal laws enumerated herein; (2) as devices used in conjunction with the collection and storage of electronic data and records related to the alleged violations and (3) fruits of illegal activity. Search and seizure of computer hardware, software, documentation, passwords, and data security devices, either as instrumentalities of criminal activity or as storage devices for evidence thereof, is contemplated for the seized electronic devices. Affiant is aware that many bank robberies are committed with an interstate nexus. The robbery described in this affidavit illustrates this interstate scope with a Tennessee bank being robbed, the escape vehicle recovered in Alabama, and the subjects who are residents of Maryland and Virginia, finally arrested in southwestern Virginia. Affiant is aware that bank robbers will plan their robberies in detail, including researching and planning the escape route. The use of Global Positioning Systems (GPS) routing systems can aid a subject in finding the shortest route of escape when they are unfamiliar with an area distant from their domicile. The use of the internet is used in the planning a bank robberies. The internet contains mapping programs such as Google Maps, Yahoo Maps, and Mapquest, that when coupled with a GPS device, can aid in the execution of a bank robbery and the escape from a bank robbery. Affiant is aware of bank robbers targeting banks located close to state lines to facilitate an escape across state lines and the jurisdiction of local and state law

enforcement officers responding to a bank hold up alarm. Affiant is aware that GPS units contain search features that contain information and the location of businesses such as banks, as stations and restaurants and hotels, and information on the location of local government offices such as police stations. The internet, when accessed by a bank robber using a computer, can provide much of the information needed to execute a successful robbery, avoid police response actions, and affect a successful escape.

Affiant believes that the laptop computers and GPS unit located in the vehicle that also contained the firearms used to commit this crime, as well as the proceeds of this crime, will contain a history of searches and files related to the routing of the escape, the identity of the bank, the location of law enforcement, search for the frequencies of law enforcement communication systems and a history of locations used by the subjects Crawley and Allen in the pre-robbery planning and post robbery escape.

Computer hardware is described as all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but is not limited to, any data-processing devices (such as central processing units, memory typewriters, self-contained "laptop" or "notebook" computers, "palm pilots," and "schedulers" and "GPS units"); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, zip disks, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

Computer software is described as digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

a. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the computer hardware, software, or other related items.

b. Computer passwords and other data security devices are described as a string of alpha-numeric characters designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

Special Agent Stephen D. McFall. "CART AGENT" with the Knoxville Division of the FBI has advised that based upon his knowledge, training and experience, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deleted" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on the particular user's operating system, storage capacity, and computer habits.

SA McFall has advised that based upon his knowledge, training and experience, and that of the CART unit, searching and

seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

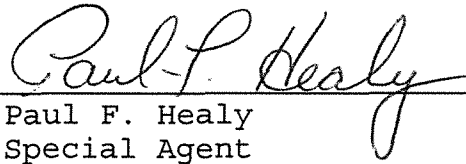
b. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of the computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

c. GPS devices may contain information such as addresses searched, routes taken, time of related activity, and other related travel information. This information is stored in the memory of the GPS device and can be extracted during a digital media examination.

In light of these concerns, your Affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described.


V. CONCLUSION

Based upon information provided in this affidavit, affiant submits there is probable cause to believe that the violations of Title 18 U.S.C. 2113(a) and (d) and Title 18 U.S.C. Section 924(c), have been committed. Accordingly, affiant seeks a search warrant for the following items: Acer laptop computer bearing serial number LXAKVOX3798080903E2503, a Dell laptop computer bearing serial number CN-03U652486433930499, and a Tomtom GPS device bearing serial number C-NO:Y25497B00279 which constitute evidence of violations against the laws of the United States.



Paul F. Healy
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me this 17 day of February, 2011:


William B. Carter
UNITED STATES MAGISTRATE JUDGE